Firmware Analysis of NetBotz (APC - Schneider Electric) Rack Monitor 570/550/450 and Wall Monitor 455/355 - 4.5.3

March 28, 2018

Meta Data

HID	NetBotz (APC - Schneider Electric) Rack Monitor 570/550/450 and Wall Monitor 455/355 - 4.5.3
Device Name	Rack Monitor 570/550/450 and Wall Monitor 455/355
Vendor	NetBotz (APC - Schneider Electric)
Device Class	DVR
Version	4.5.3
Release Date	2016-11-02
Size	21.58 MiB (22,632,490 bytes)

Analysis

base64decoder

Time of Analysis	2018-03-23 16:08:46
Plugin Version	0.1.2
Summary	

cpu architecture

Time of Analysis	2018-03-23 16:09:17
Plugin Version	0.3.1
Summary	PPC (M)

crypto material

Time of Analysis	2018-03-23 16:08:38
Plugin Version	0.5
Summary	

exploit mitigations

Time of Analysis	2018-03-23 16:09:14
Plugin Version	0.1.1
Summary	

file hashes

Time of Analysis	2018-03-23 16:09:45
Plugin Version	1.0
sha1	164eb4233b78da456232c082dcaf5a0dd4021919
ssdeep	393216:JCWk8T1ykEFKvGf+/9vFmYS678jcZOzzyHGUPccDuHiWcCWTi0PlhHa:a8TokvQ+
sha256	26ef025078abda69d2c3de06e27142a6db1a6385bd2524ce4976211570264a39
ripemd160	450c7e078958fd4b58214005acb44a7fc36c6f58
imphash	None
sha512	da38955f0df1be8e9713967c6d2e5d5d27ca1bd421e96f9159ab802b4586d8b4b1fe62dbb2092ed4b85
md5	aff3ed2821d4a3c0e1cb0a56c0048393
whirlpool	2517d24d06ac652e06bfbb32b4b1a70e899a6b0a48963e9f2262204a3e303b80f6e44c66027781ed4125

file type

Time of Analysis	2018-03-23 16:09:10
Plugin Version	1.0
File Type	`uImage header, header size: 64 bytes, header CRC: 0x759DDD, created: Fri Sep 30`
MIME	`firmware/u-boot`
Summary	firmware/u-boot

init systems

Time of Analysis	2018-03-23 16:09:19
Plugin Version	0.4.1
Summary	

ip and uri finder

Time of Analysis	2018-03-23 16:08:36
Plugin Version	0.4.1
IPv4	List is empty.
IPv6	B:: 3::b 5:: ::B ::E 6::E D:: 2::7 ::e 1:: 4:: ::5 9::D3 ::8 61::5 ::a c:: ::4 ::2D2 a:: C:: 8:: A:: ::c 83:: E2:: ::9F 7:: 02:: E:: ::F ::3 0::A ::bF 6:: :: ::d F::
URI	The List is empty.
Summary	B:: 3::b 5:: ::B ::E 6::E D:: 2::7 ::e 1:: 4:: ::5 9::D3 ::8 61::5 ::a c:: ::4

software components

Time of Analysis	2018-03-23 16:08:58
Plugin Version	0.3
Summary	

printable strings

Time of Analysis	2018-03-23 16:09:04
Plugin Version	0.2
Strings	`['\t\te\\*kY/', '\t\tzVz\r5', '\t\n8@v u"', '\t\n9J8:', '\t\nG&gN', '\t\nGRTn\\`

users and passwords

Time of Analysis	2018-03-23 16:08:51
Plugin Version	0.4
Summary	

string evaluator

Time of Analysis	2018-03-23 16:09:32
Plugin Version	0.2
Strings	`['\\)b@H.eh', '-/WJxWO[J', '-A\tLv5/q9n', '/pdR\x0bzbe\x0bLzVD7', 'I\r7#/cjDjd`

unpacker

Time of Analysis	2018-03-23 16:08:29
Plugin Version	0.1
Plugin	Uboot
Extracted	2
Output	
Size packed -> unpacked	`21.57 MiB -> 21.58 MiB`
Entropy	0.89
Summary	no data lost

malware scanner

Time of Analysis	2018-03-23 16:08:56
Plugin Version	0.3
MD5	aff3ed2821d4a3c0e1cb0a56c0048393
System Version	0.2.6
Scanners Number	1
Positives	0
Scanners	ClamAV

Scanns	`ClamAV :: result:clean`
	`ClamAV :: detected:False`
	`ClamAV :: version:ClamAV 0.99.4/24413/Fri Mar 23 13:22:23 2018`

Summary	